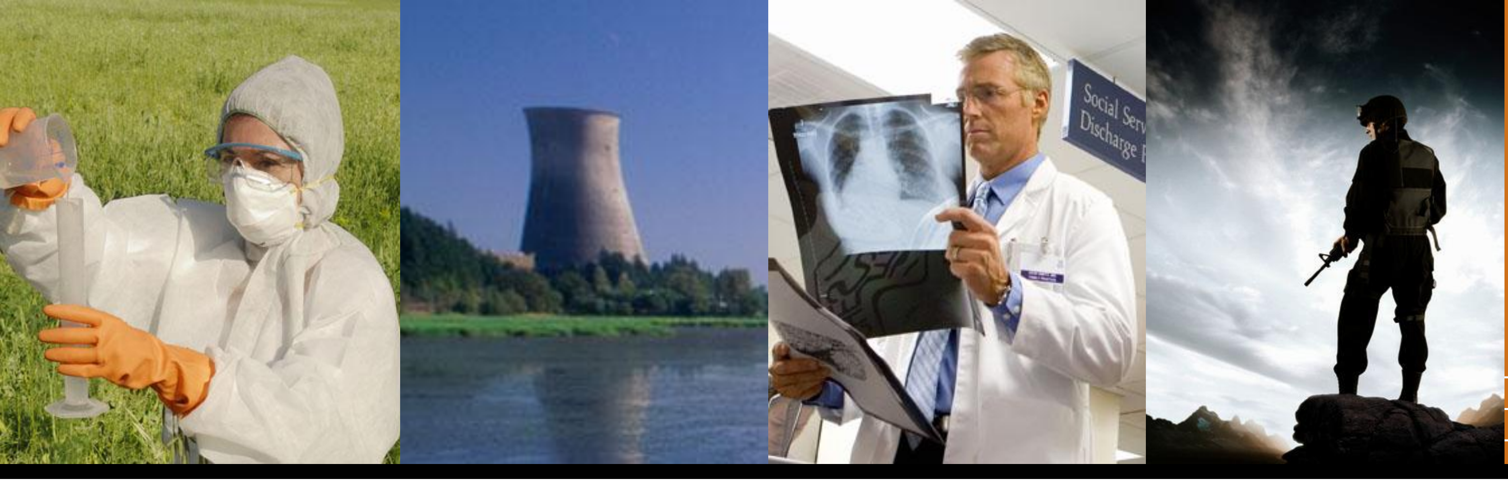


Digital I&C: Safety, Security and Availability
IAEA-CN-194-098

Third International Conference on Nuclear Power Plant Life Management (PLiM)
Salt Lake City, Utah, USA
14 to 18 May 2012

Ewald Liebhart
Manager R&D
Mirion Technologies (MGPI H&B) GmbH
Munich, Germany

MIRION TECHNOLOGIES Radiation Monitoring Systems Division

Table of Contents

1. Why digital signal processing for safety related applications

2. Advantages of digital signal processing

3. Mastering the risks of software

4. Mastering the risks of hardware

5. IT (cyber) security

6. Signal Processing System proTK^{TM} / TK 250

1. Why digital signal processing for safety related applications

- Obsolescence of analogue components (Semiconductors, integrated circuits)
  - Reduction of component variety
  - Problem of spares

- No limitation for signal processing algorithms: precision and “flexibility”
  - Calculation of logarithmic scales
  - Combination of pulse signal and Campbell signal for the wide range “overlapping”
  - Calculation & precision of alarm thresholds (gradually shifting thresholds)
  - Multiplication , e.g. flow rate
  - Calibration, flexible parameters

2. Advantages of digital signal processing

- High degree of self monitoring for HW & SW
  - low risk of hidden failures
- Simplified periodical testing, extension of test interval
  - algorithms fixed in EPROM (and continuously monitored)
  - precision and response time determined (mainly) by software (= EPROM)
  - easy check of parameters
  - remotely activated test generators for input signals
  - numerical simulation of output signals

3. Mastering the risks of software

A software failure could become a common cause failure!

- Engineering-like development of software (state of the art!)
  - Carefully planning, design, simulation, coding
  - Aim -> zero-failure software
- Limitation to essential functions
  - KISS (Keep it simple, …)
- Continuous quality assurance & real safety culture
  - The SW engineer is aware of the safety critical environment of application (i.e. nuclear)
- Verification & validation
  - Type test certified by independent expert (TÜV)
- Operational experience (see proTK^{TM} / TK 250 features)

4. Mastering the risks of hardware

- Main risk: obsolescence of components (“computer products”)
- How to deal with this risk?
  - Use of well established components; no requirements for “best performing” in terms of speed, memory size, etc (= usually latest on market).
  - Re-design of fully compatible new boards with new components
  - E.g. proTK^{TM}
    - □ on market for more than 20 years
    - □ some boards are of 2nd generation, but:
      - ○ Fully exchangeable/compatible
      - ○ Re-qualification including test of compatibility

5. IT (Cyber) Security

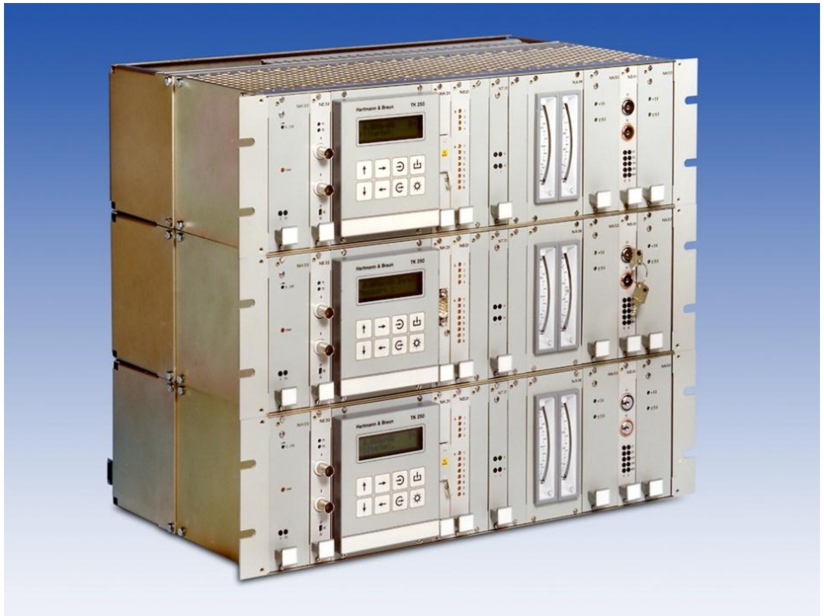
- Achieved through “progressive barrier/firewall”
  - No access for external computer,

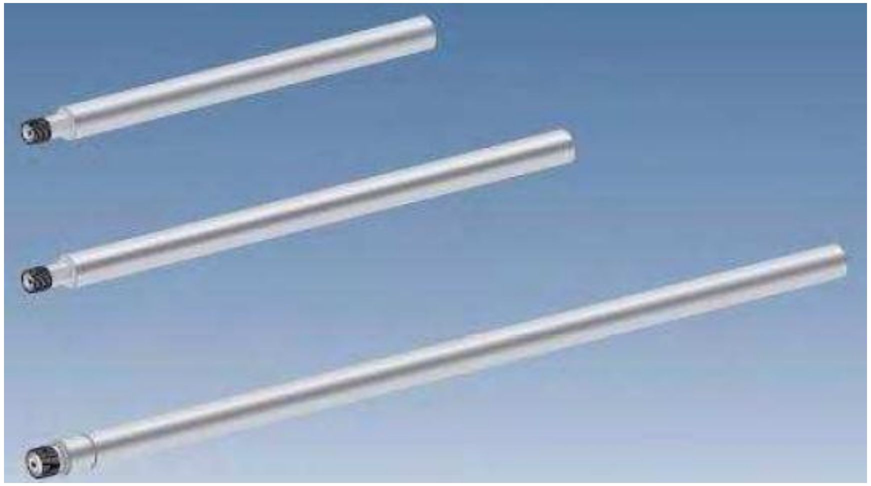
    fully manual access
  - “Read-only” parameters and results
  - Dedicated op-codes only,
    e.g. re-calibration or activation of test
  - Full access by external computer

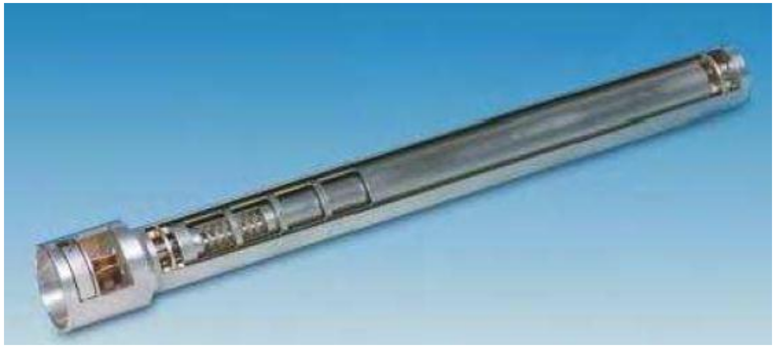
6. proTK^{TM} / TK 250 - NFMS (continued) Channel Types

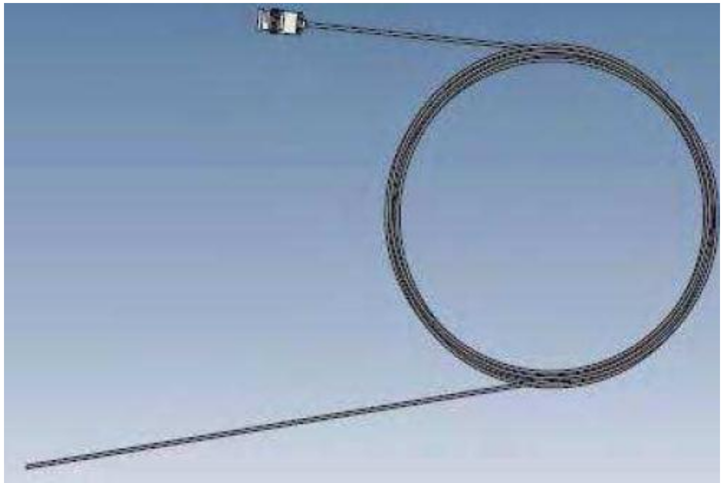
- DAK 250 - Source and Intermediate Range Monitoring
  - with pulse or DC signal processing; reactimeter optional
- DWK 250 - Wide Range Monitoring
  - combined pulse and Campbell processing for in-/out-core fission chambers
- DGK 250 - Power Range Monitoring
  - with 1 or 2 signal paths for neutron ionization chambers
- DLK 250 - Flux Distribution Monitoring
  - for 3 or 6 SPN-detectors with background compensation, calibration and noise reduction
- DSK/DMK 250 – Local/Average Power Range (BWR)
  - for average and flow related flux with stability monitoring

6. proTK$^{\mathrm{TM}}$ / TK 250 - NFMS (continued) Digital Channel & Detectors





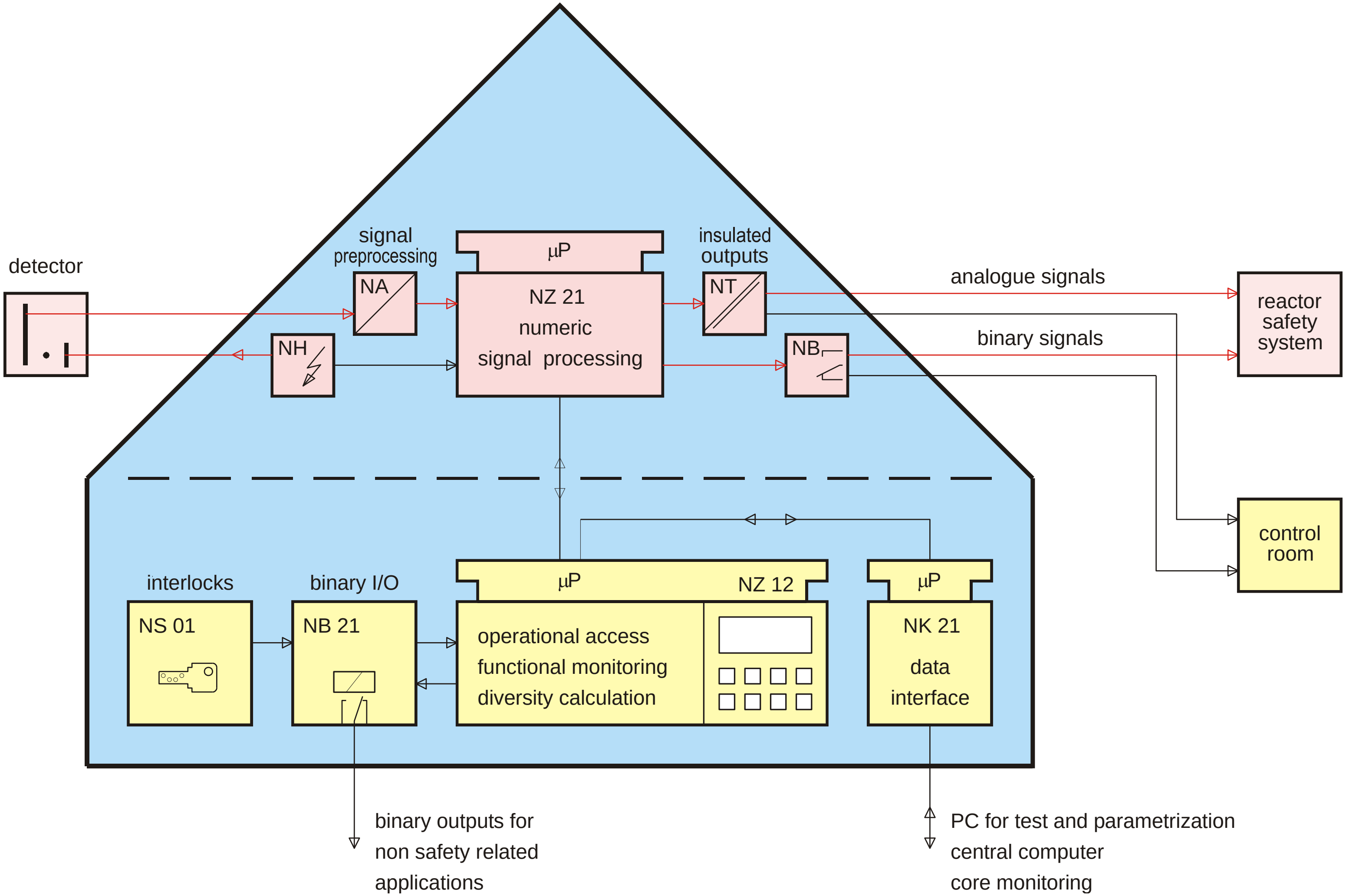




6. proTK™ / TK 250 - NFMS (continued) Features

• Modular system – easy to adapt into an existing plant	**Flexible**
• Signal processing software fixed in EPROM	**Safe**
• Remote test signals, electrical & digital	**Verifiable / Testable**
• Designed and type tested – according to KTA and IEC standards	**Qualified**
• Long operational experience	**Reliable**

6. proTK™ / TK 250 - NFMS (continued)
System Architecture



Mirion offers an array of solutions and services for managing radiological hazards.

Learn more at: **www.mirion.com**

MIRION TECHNOLOGIES

Radiation Monitoring Systems Division

6. proTK^{TM} / TK 250 - NFMS (continued) System Design – Clear & Simple

- **The functions for the safety signal path are concentrated on the independent I/O-micro-processor board NZ 21:**
  - **The software is purely sequential and deterministic**
  - **The software operates cyclic in a fixed time grid, e.g. 10 ms**
  - **Therefore, the response time is predictable**
  - **There is no operating system**
  - **The volume of the software is as small as 3 to 8 kByte**
- **All other functions e.g. operator’s access or self monitoring are allocated on the “main processor board” NZ 12**
- **Re-use of type-tested and proven software modules**
- **The target: zero-fault software**
  - **Designed and developed by well-trained engineers**
  - **Verified by typetest of independent experts (TÜV)**
  - **True proven by long-term operational experience**

6. proTK^{TM} / TK 250 - NFMS (continued) System Design – “Defeating” CCF

- **Measures against CCF of the software**
  - **Additional to the simple and clear design there is:**
    - **No use of interrupts on NZ 21, only 1 timer interrupt on NZ 12**
    - **No use of real time clock or calendar**
    - **NZ 12 has no direct access to NZ 21 and its**
      - ✓ **Program sequence**
      - ✓ **Data or parameter memory**
    - **NZ 21 is hardware-locked by key switch against access to parameters and test-procedures (DGK & DMK 250)**
    - **A variety of self monitoring devices, some of them complementary between NZ 12 and NZ 21**

6. proTK^{TM} / TK 250 - NFMS (continued) System Design – Self Monitoring

- A variety of items is used to detect faults of hardware and software, e.g. monitoring of internal voltages, arithmetics, time schedule, micro-processors, transfer of data, data and program memory. Additional, there are two very efficient tools:

  - NZ 12 performs a “re-calculation” of the results
    - ✓ Using a snapshot of data transferred from NZ 21
    - ✓ Using a different software and arithmetic package (e.g. floating point package instead of fixed point arithmetics)
    - ✓ Comparing the results and generating an alarm if necessary

  - A cycle counter on NZ 21 is interpreted periodically by NZ 12
    - ✓ The differences of two readings are compared with setpoints
    - ✓ NZ 12 & NZ 21 are monitoring their cycle times one another
    - ✓ The response of NZ 12 is additionally monitored by a watch dog

6. proTK^{TM} / TK 250 - NFMS (continued)
System Design – Self-Checks & Tests

- **Different tools make periodical testing efficient but easy:**
  - **Test generators in pre-amps or input-boards of the channel:**
    - ✓ **May be activated remotely without manipulation in the wiring**
    - ✓ **Insert a reference signal to the input of the electronic channel**
  - **The tool “simulation” enables to:**
    - ✓ **Insert arbitrary numbers at defined points of the signal path**
    - ✓ **Generate all desired output values for analog signals or alarms**
  - **Binary outputs (relays) may be activated or deactivated**
  - **All testing tools are locked by key-switch and generate a flag signal**
  - **The basic procedure for periodical testing**
    - ✓ **Is described in the user manual**
    - ✓ **Was checked by TÜV during type test**

6. proTK^{TM} / TK 250 - NFMS (continued)
System Design – Type Testing

- The type test of hardware was performed according to KTA 3505
  - Theoretical and practical tests observed and checked by TÜV
  - Test results transferable to IEEE 323 or IEC 60780
  - Data of operational experience for all boards available
- Software type test also was performed by independent experts:
  - DAK, DGK, DLK 250 and all other channels by TÜV-Nord/Hamburg
  - IEC 880 was applied for DAK, DGK and DLK 250, elements of FMEA
  - Result: the software is qualified for the use in the level of RPS
- Finally an integration test of hardware and software was performed:
  - e.g. functions, characteristics, dynamic response, EMC
  - Some tests also under worst-case conditions

6. proTK^{TM} / TK 250 - NFMS (continued) System Design – Operator Access

- **The access to parameters and testing is locked by 2 key switches**
  - **Without key: parameters may be displayed, but not modified**
  - **DGK 250 additionally has a separated access to re-calibration**
- **A parameter protocol may be generated on a PC via serial interface using purely read-only instructions**
- **The variety of functions and parameters is limited by “configuration” according to customer/project requirements:**
  - **Delete (enable and hide) unused functions**
  - **Establish “fixed parameters”, e.g. scalings or trip thresholds**
  - **Use of modified text tables, e.g. language version**
  - **Configuration is done by Mirion Technologies and checked by TÜV**
  - **Configuration data are stored in EPROM**

6. proTK^{TM} / TK 250 - NFMS (continued) Installations - NPPs

Country	Name/Unit(s)	Type	Year(s)	Installed Channel(s)/Module(s)
CH	Mühleberg	BWR	1994	WRM
CH	Beznau-1/2	PWR	1997…	WRM
DE	Würgassen	BWR	1989…	WRM, LPRM, APRM
DE	Philippsburg-1	BWR	1993/94, 2003…	LPRM/APRM, WRM
DE	Philippsburg-2	PWR	2005/09	SRM, IRM, PRM, N16
DE	Obrigheim	PWR	1995/96	SRM, IRM, PRM, N16
DE	Krümmel	BWR	1997...	WRM, LPRM, APRM
DE	Isar-1	BWR	2000, 2007	WRM, LPRM, APRM
DE	Neckarwesth.-1/2	PWR	2008/2009	SRM, IRM, PRM
B	Doel 3/4, Tihange 2/3	PWR	from 2012	SRM, IRM, PRM
SK	Bohunice	VVER	1997 …	Input boards for WRM
HU	Paks	VVER	1998 …	Input boards for WRM
S	Oskarshamn	BWR	1998 ...	Input boards for WRM and LPRM

Legend: see next page

6. proTK^{TM} / TK 250 - NFMS (continued) Installations - TRTR

Country	Name / Short	Year	Installed Channel(s)
DE	Berlin, Research Reactor / HMI	1999…	SRM, IRM, PRM, N16
DE	Garching, Research R. / FRM-2	2000	WRM
DE	Geesthacht, Research R. / GKSS	2001…	SRM, IRM, PRM
DE	Dresden, Training Reactor / AKR-2	2003…	SRM, IRM
NL	TU-Delft, Research R. / HOR	2010	SRM, IRM, PRM, RMS
US	NIST (Center for Neutr. Res.) / NCNR	2012	SRM
US	MIT Nuclear Reactor Lab. / MITR-II	2012	WRM

Legend

DE	Germany	**SRM**	Source / Start-up Range Monitor	**BWR**	Boiling Water Reactor
CH	Switzerland	**IRM**	Intermediate Range Monitor	**PWR**	Pressurized Water Reactor
B	Belgium	**PRM**	Power Range Monitor	**VVER**	Russian Pressurized Water Reactor
NL	Netherlands	**WRM**	Wide Range Monitor		
US	USA	**LPRM**	Local Power Distribution Monitor		
SK	Slovakia	**APRM**	Average Power Monitor		
HU	Hungary	**N-16**	N-16 Process Monitor		
S	Sweden				

6. proTK^{TM} / TK 250 - NFMS (continued) Summary Operational Experience

• Number of channels in operation	> 280
• Number of reactors	> 20
• Total number of years in operation	> 3,000 years
• Average MTBF of the electronic boards	4,000,000 hours
• Total number of software failures	0

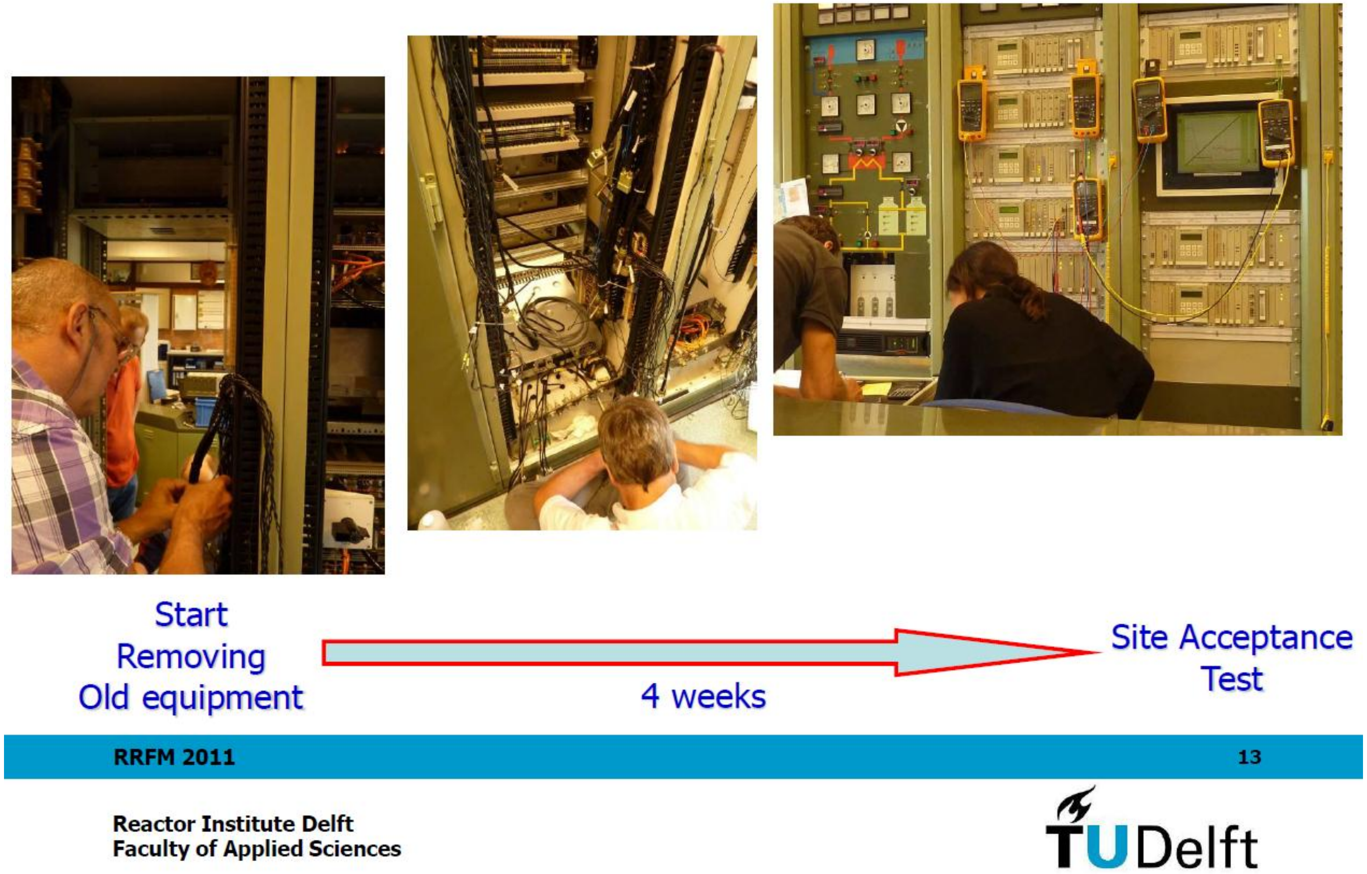
6. proTK^{TM} / TK 250 - NFMS (continued)

Refurbishment Project HOR@TU Delft

Picture from http://tnw.tudelft.nl/

6. proTK^{TM} / TK 250 - NFMS (continued)

Refurbishment Project HOR@TU Delft



Start
Removing
Old equipment

4 weeks

Site Acceptance
Test

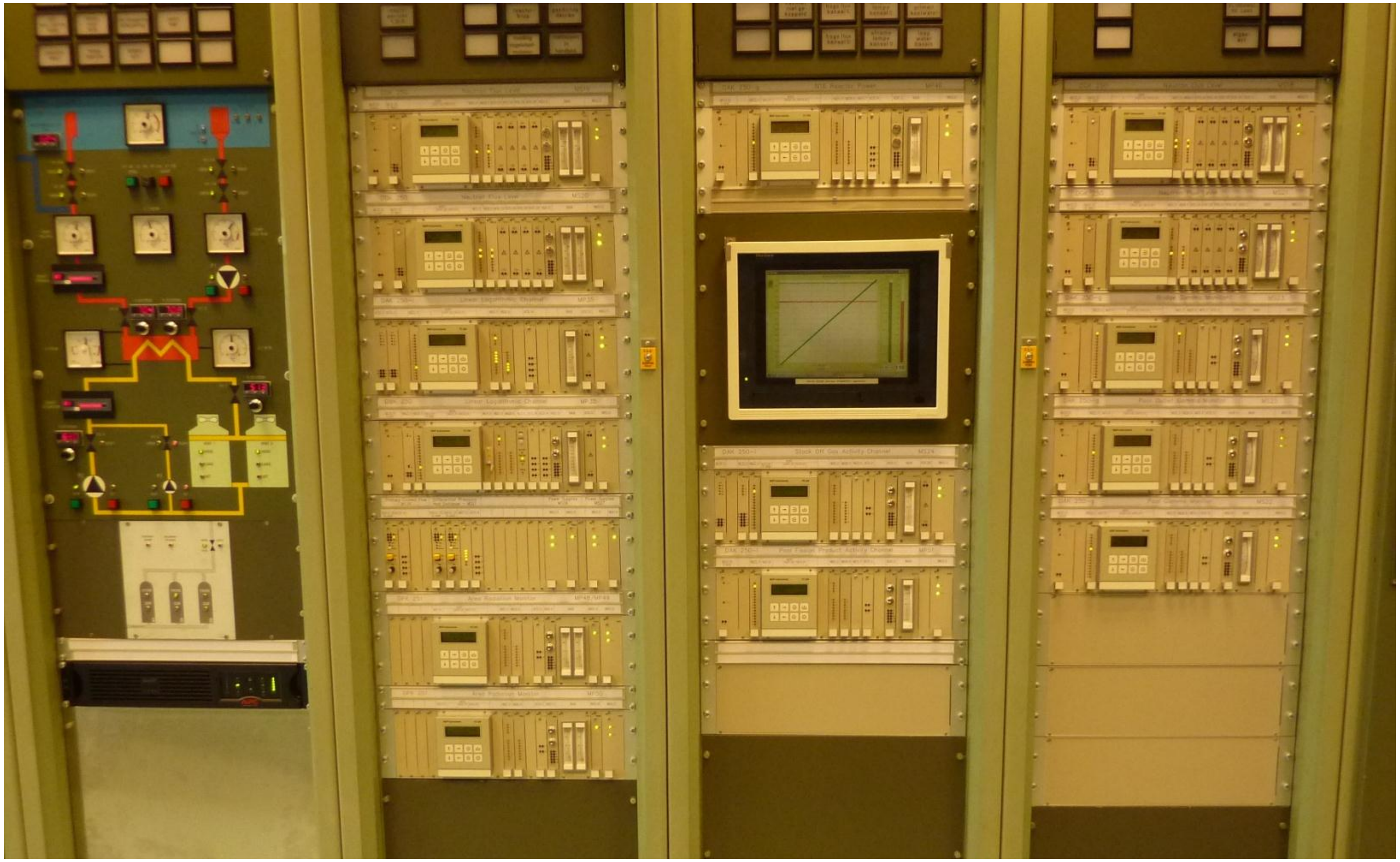
RRFM 2011 13

Reactor Institute Delft
Faculty of Applied Sciences

By courtesy of
C.N.J. Kaaijk, Presentation at RRFM 2011, Rome (Italy)

6. proTK^{TM} / TK 250 - NFMS (continued)

Refurbishment Project HOR@TU Delft



Summary

- Advantages of digital signal processing
  - Increased performance (adaptability, flexibility , functionality)
  - Improved safety, reliability & availability
  - Reduced overall “life cycle” cost
- IT (cyber) security risks can be managed
  - “Progressive” barrier/firewall according to needs
- Digital signal processing channels TK 250
  - Offer all the advantages of a digital signal processing system
  - Proven reliability through more than 3000 operation years, achieved with more than 280 installed channels

Thank you for you attention!

Third International Conference on Nuclear Power Plant Life Management (PLiM)
Salt Lake City, Utah, USA
14 to 18 May 2012

Ewald Liebhart
Manager R&D
Mirion Technologies (MGPI H&B) GmbH
Munich, Germany

eliebhart@mirion.com